

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-339227

(43)Date of publication of application : 08.12.2000

(51)Int.Cl.

G06F 12/14
G06T 1/00
H04N 1/387

(21)Application number : 11-147769

(71)Applicant : FUJITSU LTD

(22)Date of filing : 27.05.1999

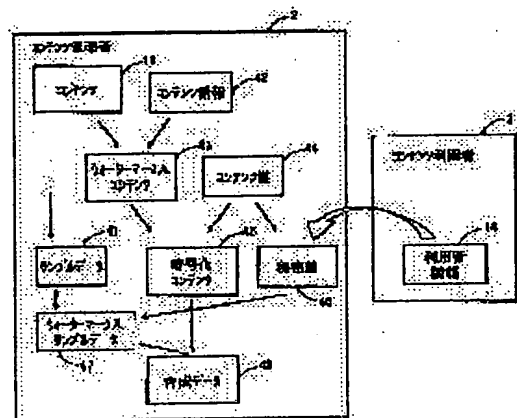
(72)Inventor : HIRANO HIDEYUKI
KOTANI MASATAKE
HASHIMOTO SHINJI

(54) DATA OPERATING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent piracy by distributing digital contents by ciphering them and to prevent destruction and loss of permission information to decode the ciphered digital contents.

SOLUTION: The ciphered contents 45 is generated by ciphering the digital contents 11 by a contents key 44, a part of the digital contents 11 is extracted as sample data 41, sample data 47 with watermark formed by embedding a secret key 46 formed by ciphering the contents key 44 by user information 14 in the sample data 41 as invisible information is generated and synthetic data 48 formed by synthesizing the ciphered contents 45 with the sample data 47 with watermark is distributed.



LEGAL STATUS

[Date of request for examination]

13.12.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-339227
(P2000-339227A)

(43) 公開日 平成12年12月8日 (2000. 12. 8)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコード*(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
G 0 6 T 1/00		H 0 4 N 1/387	5 B 0 5 7
H 0 4 N 1/387		G 0 6 F 15/66	B 5 C 0 7 6

審査請求 未請求 請求項の数17 O L (全 9 頁)

(21) 出願番号 特願平11-147769

(22) 出願日 平成11年5月27日 (1999. 5. 27)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 平野 秀幸

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 小谷 誠剛

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 100094145

弁理士 小野 由己男 (外2名)

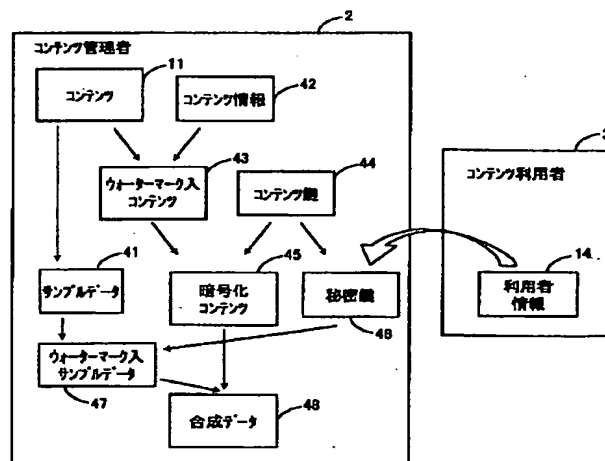
最終頁に続く

(54) 【発明の名称】 データ運用方法

(57) 【要約】

【課題】 デジタルコンテンツを暗号化して配布することで著作権の侵害を防止し、かつ暗号化されたデジタルコンテンツを復号化するための許諾情報が破壊されたり、紛失したりすることを防止するデータ運用方法を提供する。

【解決手段】 デジタルコンテンツ11をコンテンツ鍵44によって暗号化して暗号化コンテンツ45を作成し、デジタルコンテンツ11の一部をサンプルデータ41として抽出し、コンテンツ鍵44を利用者情報14によって暗号化した秘密鍵46をサンプルデータ41に不可視情報として埋め込んだウォーターマーク入サンプルデータ47を作成し、これに暗号化コンテンツ45を合成した合成データ48を配布する。



1

【特許請求の範囲】

【請求項 1】配布を行うデジタルコンテンツを暗号化して実データ部を作成し、

前記デジタルコンテンツの一部をサンプルデータとして抽出し、前記サンプルデータに前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を不可視情報として埋め込んだサンプルデータ部を作成し、

前記実データ部と前記サンプルデータ部とを合成した合成データを作成してこれを配布するデータ運用方法。

【請求項 2】前記サンプルデータ部から許諾情報を分離し、前記許諾情報から前記実データ部を復号化するためのコンテンツ鍵を復元し、このコンテンツ鍵を用いて前記実データ部を元のデジタルコンテンツに復号化して利用することを可能とした、請求項 1 に記載のデータ運用方法。

【請求項 3】前記サンプルデータは、前記デジタルコンテンツ中に含まれる画像データに画像処理、リサイズ、圧縮またはγ補正のうち少なくとも 1 つの処理を施した画像データである、請求項 1 または 2 に記載のデータ運用方法。

【請求項 4】前記サンプルデータは、前記実データ部を代表する見出しデータである、請求項 1 ～ 3 のいずれかに記載のデータ運用方法。

【請求項 5】前記合成データは、複数のデジタルコンテンツに基づく複数の実データ部と、前記複数の実データ部に対応する複数のサンプルデータ部とを含み、前記複数のサンプルデータ部を構成する各サンプルデータはそれぞれ前記複数の実データ部の対応するものとリンクしている、請求項 4 に記載のデータ運用方法。

【請求項 6】前記サンプルデータ部は J P E G や M P E G などの構造化データであり、前記サンプルデータ部のフォーマットを利用して、前記サンプルデータ部に前記実データ部を追加合成することによって前記合成データを作成する、請求項 1 ～ 5 のいずれかに記載のデータ運用方法。

【請求項 7】前記許諾情報は、ユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載された C P U の識別情報または前記デジタルコンテンツを格納する記録媒体に固有の識別情報のうちから少なくとも 1 つを暗号鍵として、前記コンテンツ鍵を暗号化したものである、請求項 1 ～ 6 のいずれかに記載のデータ運用方法。

【請求項 8】前記許諾情報は、複数のユーザに共通な識別情報を暗号鍵として、前記コンテンツ鍵を暗号化したものである、請求項 1 ～ 6 のいずれかに記載のデータ運用方法。

【請求項 9】前記許諾情報は、前記デジタルコンテンツの配布者固有の識別情報または前記デジタルコンテンツの著作者固有の識別情報のうち少なくとも 1 つを暗号鍵

2

として、前記コンテンツ鍵を暗号化したものである、請求項 1 ～ 6 のいずれかに記載のデータ運用方法。

【請求項 10】前記暗号化されたコンテンツ鍵を復号化するための復号鍵は、暗号化を行う暗号鍵と共通であり、ユーザとコンテンツの配布者間で送受信する一意な情報に基づく共通鍵である、請求項 7 ～ 9 のいずれかに記載のデータ運用方法。

【請求項 11】前記デジタルコンテンツの配布者は、秘密鍵を用いて前記コンテンツ鍵を暗号化し、ユーザは前記デジタルコンテンツの配布者から予め提供されている公開鍵を用いて前記暗号化されたコンテンツ鍵を復号化する、請求項 7 ～ 9 のいずれかに記載のデータ運用方法。

【請求項 12】前記サンプルデータ部は、ユーザが前記デジタルコンテンツを利用した利用回数を不可視情報として備え、ユーザが前記デジタルコンテンツを利用する毎に前記不可視情報を書き換えることを特徴とする、請求項 1 ～ 11 のいずれかに記載のデータ運用方法。

【請求項 13】前記サンプルデータ部は、利用回数制御を可能とする許諾情報を不可視情報として備え、ユーザが前記デジタルコンテンツを所定回数以上利用した際に、前記不可視情報を書き換えることを特徴とする、請求項 1 ～ 11 のいずれかに記載のデータ運用方法。

【請求項 14】前記実データ部を復号化して読み込む際またはデジタルコンテンツ利用終了時に、前記不可視情報を書き換えることを特徴とする、請求項 12 または 13 に記載のデータ運用方法。

【請求項 15】前記サンプルデータ部の不可視情報は、冗長情報を含むことによりエラー回復機能を備える、請求項 12 ～ 14 のいずれかに記載のデータ運用方法。

【請求項 16】前記実データ部を復号化する際に、前記サンプルデータ部の不可視情報に基づいて再生する範囲を規制することを特徴とする、請求項 12 または 13 に記載のデータ運用方法。

【請求項 17】前記実データ部を復号化する際に、前記サンプルデータ部の不可視情報に基づいて再生できる年、月、日、時間のいずれかの範囲を規制することを可能とする、請求項 12 または 13 に記載のデータ運用方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ運用方法に関し、特に、デジタルコンテンツを特定の許諾情報で暗号化して配布する際のデータ運用方法に関する。

【0002】

【従来の技術】コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク (MO)、デジタルビデオディスク (DVD)、フロッピーディスク (FD)、ミニディスク (MD)、その他の記録媒体上に電子化データを格納して販売される。このような電子

3

化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【0003】また、インターネットやCATV、その他のネットワークなどを通じて配布される静止画像データ、動画データを含む電子化データについても同様に不正コピーが頻繁に行われ、著作権者の利益が損なわれている。このような記録媒体上に格納された電子化データや各種ネットワークを通じて配布される電子化データなどのいわゆるデジタルコンテンツを保護するために、暗号鍵を用いてデジタルコンテンツを暗号化しこの暗号化された実データを配布することが行われる。

【0004】たとえば、ユーザが自分のパーソナルコンピュータからコンテンツの配布者側にアクセスを行い、デジタルコンテンツをハードディスク上にダウンロードを行ってこれを利用する場合を考える。まず、ユーザはホストコンピュータにアクセスしてダウンロードのためのプラグインモジュールを入手する。この後、使用しているハードディスクドライブの識別番号、使用しているコンピュータのCPU識別番号、その他ユーザ固有の識別情報をホストコンピュータ側に送付する。

【0005】コンテンツの配布者側では、デジタルコンテンツをコンテンツ鍵で暗号化した実データと、コンテンツ鍵をユーザ固有の識別情報で暗号化した許諾情報を、ユーザ側に送信する。ユーザ側では、送られてきた暗号化実データと、許諾情報とを暗号化された状態のままハードディスクに記録する。デジタルコンテンツを利用する場合には、ハードディスクドライブの識別番号などのユーザ固有の識別情報を用いて、許諾情報を復号化し、コンテンツ鍵を取得する。このコンテンツ鍵を用いて、暗号化されたデジタルコンテンツを復号化してこれを利用する。

【0006】この場合、ユーザ個々にデジタルコンテンツの利用権を与える際に、デジタルコンテンツを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【0007】

【発明が解決しようとする課題】上述の方法でデータの配布を行う場合、データ配布者は暗号化されたデジタルコンテンツと、暗号化されたデジタルコンテンツの復号鍵となる許諾情報とを別々に送付する必要がある。また、ユーザ側においても、送付されてくる暗号化されたデジタルコンテンツとその許諾情報とを別々に記録媒体に格納しておく必要がある。

【0008】したがって、データ配布者側からユーザ側に送付される途中で許諾情報が破壊されたり、またはユーザ側の記録媒体上で許諾情報がなんらかの事故により破壊もしくは紛失した場合には、デジタルコンテンツを

4

利用することができなくなり、再度許諾情報入手する手順が必要となる。本発明は、デジタルコンテンツを暗号化して配布することで著作権の侵害を防止し、かつ暗号化されたデジタルコンテンツを復号化するための許諾情報が破壊されたり、紛失したりすることを防止するデータ運用方法を提供する。

【0009】

【課題を解決するための手段】本発明に係るデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの一部をサンプルデータとして抽出し、サンプルデータにデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を不可視情報として埋め込んだサンプルデータ部を作成し、実データ部と前記サンプルデータ部とを合成した合成データを作成してこれを配布する。

【0010】配布されたデジタルコンテンツを利用する場合には、サンプルデータ部から許諾情報を分離し、許諾情報から実データ部を復号化するためのコンテンツ鍵を復元し、このコンテンツ鍵を用いて実データ部を元のデジタルコンテンツに復号化して利用する。このことにより、実データ部とサンプルデータ部に不可視情報として埋め込まれた許諾情報とが一体化されており、実データ部を復号化するための許諾情報が破壊されたり紛失したりすることを防止できるとともに、この一体化されたデータを流通させることによりデータの配布が可能となるため、システムをコンパクトにすることができる。

【0011】サンプルデータは、デジタルコンテンツに含まれる画像データに画像処理、リサイズ、圧縮またはγ補正のうち少なくとも1つの処理を施した画像データとすることができる。また、サンプルデータは実データ部を代表する見出しデータとすることができる。

【0012】さらに、合成データは、複数のデジタルコンテンツに基づく複数の実データ部と、複数の実データ部に対応する複数のサンプルデータ部とを含み、複数のサンプルデータ部を構成する各サンプルデータはそれぞれ複数の実データ部の対応するものとリンクするように構成できる。また、サンプルデータ部はJPEGやMP EGなどの構造化データであり、サンプルデータ部のフォーマットを利用して、サンプルデータ部に実データ部を追加合成することによって合成データを作成するように構成できる。

【0013】許諾情報は、ユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載されたCPUの識別情報またはデジタルコンテンツを格納する記録媒体に固有の識別情報のうちから少なくとも1つを暗号鍵として、コンテンツ鍵を暗号化したものとして、複数のユーザに共通な識別情報を暗号鍵として、コンテンツ鍵を暗号化したものとしても可能であり、さらに、デジタル

5

コンテンツの配布者固有の識別情報またはデジタルコンテンツの著作者固有の識別情報のうち少なくとも1つを暗号鍵として、コンテンツ鍵を暗号化したものとすることもできる。

【0014】暗号化されたコンテンツ鍵を復号化するための復号鍵は、暗号化を行う暗号鍵と共通であり、ユーザとコンテンツの配布者間で送受信する一意な情報に基づく共通鍵とすることができる。また、デジタルコンテンツの配布者は、秘密鍵を用いてコンテンツ鍵を暗号化し、ユーザはデジタルコンテンツの配布者から予め提供されている公開鍵を用いて暗号化されたコンテンツ鍵を復号化するように構成することも可能である。

【0015】また、サンプルデータ部は、ユーザがデジタルコンテンツを利用した利用回数を不可視情報として備え、ユーザがデジタルコンテンツを利用する毎に不可視情報を書き換えるように構成できる。さらに、サンプルデータ部は、利用回数制御を許諾情報を不可視情報として備え、ユーザがデジタルコンテンツを所定回数以上利用した際に、不可視情報を書き換えるように構成できる。

【0016】この場合、実データ部を復号化して読み込む際またはデジタルコンテンツ利用終了時に、不可視情報を書き換えるように構成できる。また、サンプルデータ部の不可視情報は、冗長情報を含むことによりエラー回復機能を備える構成とすることができる。実データ部を復号化する際に、サンプルデータ部の不可視情報に基づいて再生する範囲を規制するように構成でき、実データ部を復号化する際に、サンプルデータ部の不可視情報に基づいて再生できる年、月、日、時間のいずれかの範囲を規制するように構成できる。

【0017】

【発明の実施の形態】〔発明の概要〕図1に本発明の概要構成を示す。コンテンツ提供者1は、デジタルコンテンツの著作者、版權者などであり、運用を行うデジタルコンテンツ11をコンテンツ管理者2に提供する。

【0018】コンテンツ管理者2は、コンテンツ提供者1から提供されるデジタルコンテンツ11を運用するために暗号化し、この暗号鍵を管理するとともに、このデジタルコンテンツ11を利用するユーザの利用者情報を管理する。コンテンツ利用者3は、コンテンツ管理者2が管理しているデジタルコンテンツを利用したい場合には、利用者情報14をコンテンツ管理者2に送信する。

【0019】コンテンツ管理者2は、コンテンツ利用者3から送信された利用者情報14を管理するとともに、この利用者情報14に基づくコンテンツ使用許諾情報13を作成し、暗号化コンテンツ12と一体化してコンテンツ利用者3に送信する。このとき、コンテンツ管理者2はデジタルコンテンツ11からコンテンツの内容を代表するようなサンプルデータを抽出する。デジタルコンテンツ11を暗号化した暗号鍵を利用者情報14によ

6

て暗号化してコンテンツ使用許諾情報13を作成し、これをサンプルデータ中に不可視情報として埋込んだサンプルデータ部を作成する。さらに、このサンプルデータ部を暗号化コンテンツ12と合成してコンテンツ利用者3に送信する。このとき、コンテンツ提供者1とコンテンツ管理者2は同一であってもよい。

【0020】〔コンテンツ管理者〕コンテンツ管理者2側の概略構成を示す機能ブロック図を図2に示す。このコンテンツ管理者2側では、運用を行うコンテンツを管理するコンテンツ管理部21、所定のコンテンツ鍵を用いてデジタルコンテンツを暗号化するコンテンツ暗号化部22、コンテンツ鍵を管理するコンテンツ鍵管理部23、コンテンツ利用者3の利用者情報を取得してこれを管理する利用者情報管理部24、利用者情報管理部24で管理している利用者情報情報に基づいてデジタルコンテンツの利用許諾情報を作成しこれを管理する許諾情報管理部25、デジタルコンテンツからサンプルデータを抽出しこれに許諾情報を不可視情報として埋め込む許諾情報入サンプル作成部26、コンテンツ鍵を用いて暗号化した暗号化コンテンツと許諾情報入サンプルデータとを合成する暗号化コンテンツ合成部27などを備えている。

【0021】〔コンテンツ利用者〕コンテンツ利用者3側の概略構成を示す機能ブロック図を図3に示す。このコンテンツ利用者3側では、使用しているハードディスクドライブの識別番号、コンピュータに搭載されているCPUの識別番号、その他の利用者固有の識別情報を管理する利用者情報管理部31、コンテンツ管理者2からの合成データを取得するための合成データ取得部32、取得した合成データのうちサンプルデータを表示するためのサンプルデータ表示部33、許諾情報入サンプルデータから許諾情報を分離する許諾情報抽出部34、抽出した許諾情報を復号化してコンテンツ鍵を再生するコンテンツ鍵復号部35、復号化されたコンテンツ鍵を用いて暗号化コンテンツを復号化するコンテンツ復号部36、復号化したデジタルコンテンツを動作させるコンテンツ動作部37などを備えている。

【0022】〔コンテンツ配布〕デジタルコンテンツを配布する際にコンテンツ管理者2側が行う動作を図4、図5に基づいて説明する。デジタルコンテンツ11は、そのコンテンツ情報42が電子透かし（ウォーターマーク）として埋め込まれてウォーターマーク入コンテンツ43となる。ここでは、データの特定の周波数帯域にコンテンツ情報42を挿入するように構成でき、またデータの一部を間引きし、ここにコンテンツ情報42を挿入するように構成することもできる。コンテンツ情報42は、たとえばこのデジタルコンテンツ11の著作権情報とすることができ、このような情報の埋込を省略することも可能である。

【0023】ステップS1では、コンテンツ鍵44を用

7

いてウォーターマーク入コンテンツ43を暗号化し、暗号化コンテンツ45を作成する。ステップS2では、利用者情報14を獲得する。ここでは、コンテンツ利用者2側からアクセスがあった場合に、コンテンツ利用者2が使用しているハードディスクドライブの識別番号、コンピュータに搭載されているCPUの識別番号などのコンテンツ利用者3に固有の識別情報を送信させ、これを利用者情報管理部24（図2参照）に格納しておく。

【0024】ステップS3では、獲得した利用者情報14を用いてコンテンツ鍵44を暗号化し、秘密鍵46を10作成する。この秘密鍵46は、コンテンツ利用者3に固有の利用者情報14に基づいて暗号化されているため、このデジタルコンテンツ11を利用するための許諾情報となっている。ステップS4では、デジタルコンテンツ11からこのコンテンツを代表するようなデータをサンプルデータ41として抽出する。デジタルコンテンツ11が複数の画像データを含む場合、このうちの1つの画像データをサンプルデータ41として抽出することができる。複数のデジタルコンテンツ11を同時に運用する場合には、ここで抽出したサンプルデータ41を対応するデジタルコンテンツ11とリンクさせ、複数のサンプルデータのうちから所望のものを選択させ、利用するデジタルコンテンツを選ぶことができるように構成できる。

【0025】ステップS5では、サンプルデータ41に秘密鍵46を電子透かしとして埋め込んでウォーターマーク入サンプルデータ47を作成する。このウォーターマーク入サンプルデータ47は、前述と同様に、データの特定の周波数帯域に秘密鍵46のデータを挿入するように構成でき、またデータの一部を間引きし、ここに秘密鍵46のデータを挿入するように構成することもできる。このことにより、許諾情報が不可視情報として埋め込まれた許諾情報入サンプルデータが作成されたこととなる。

【0026】ステップS6では、暗号化コンテンツ45とウォーターマーク入サンプルデータ47とを合成して合成データ48を作成する。デジタルコンテンツ11が複数の画像データよりなる場合には、サンプルデータをJPEGなどの構造化データ形式にしてデータを配布することができる。この場合、サンプルデータ41とデジタルコンテンツ11をペアとし、コンテンツ毎に許諾情報を埋め込んでウォーターマーク入りサンプルデータ47を作成し、デジタルコンテンツ11をサンプルデータ47に追加合成する。

【0027】このときのJPEGデータ構造を図8に示す。ウォーターマーク入サンプルデータ47は、イメージデータの始点(SOI)63、イメージデータの終点(EOI)65および始点63と終点65に挟まれるフレーム64とからなるサンプルデータ部61として構成されている。また、コンテンツ鍵44で暗号化されたデジタルコ

8

ンテンツ66が実データ部62を構成し、このサンプルデータ部61および実データ部62が一体的に合成されている。

【0028】ステップS7では、コンテンツ利用者3の要望に応じて合成データ48を送信する。各種ネットワークなどを通じて配信する場合には、合成データ48をそのネットワークを通じて送信することとなるが、CD-ROM、DVD、その他の記録媒体に記録してこれを配布することも可能である。

【0029】〔コンテンツ利用〕コンテンツ利用者3が配布されたデジタルコンテンツを利用する場合の動作を図6、図7に基づいて説明する。ステップS21では、コンテンツ管理者2から合成データ48を取得する。このとき、コンテンツ利用者3は、予めコンテンツ管理者2側にアクセスを行い、コンテンツ管理者2が管理しているデジタルコンテンツを利用した旨を伝え、利用者固有の利用者情報14をコンテンツ管理者2側に送っているものとする。合成データ48は、各種ネットワークを通じてデータをダウンロードして得る形態であってもよく、またコンテンツ管理者2から記録媒体に記録された状態で配布されることによって得るような形態であってもよい。取得した合成データ48は、コンテンツ利用者3が使用しているハードディスク、その他の記録媒体上に格納される。

【0030】ステップS22では、合成データ48のうちからウォーターマーク入サンプルデータ50を表示させる。合成データ48内に複数のデジタルコンテンツを含む場合には、各デジタルコンテンツに対応するウォーターマーク入サンプルデータ47を縮小して並べたり、スクロールや切替などで順次表示させることでカタログ表示機能を持たせることが可能であり、クライアントソフト側でこのような機能を持たせることができる。合成データ48内に1つのデジタルコンテンツしか存在しない場合であっても、いくつかのサンプルデータを抽出してサンプルデータ部を構成し、これをカタログ表示させるように構成することも可能である。もちろん、サンプルデータがひとつの場合にはこれをそのまま表示するように構成できる。ステップS23では、コンテンツ利用者3による利用要求があったか否かを判別する。ウォーターマーク入サンプルデータ50の表示において、コンテンツ利用者3が特定のサンプルデータを選択してこれを利用する旨の指示を行った場合には、ステップS24に移行してコンテンツ利用ソフトを動作させる。

【0031】ステップS24では、合成データ48のウォーターマーク入サンプルデータ47から許諾情報を分離する。ここでは、ウォーターマーク入サンプルデータ47にウォーターマークとして埋め込まれている秘密鍵46を取り出す。秘密鍵46がサンプルデータの周波数成分として埋め込まれている場合には、ウォーターマーク入サンプルデータ47を周波数解析することにより秘

9

密鍵46を取り出すことができる。また、サンプルデータを間引きしてウォーターマークを埋め込んだ場合などの物理的埋込みが行われている場合には、画像解析を行って秘密鍵46を取り出すことが可能となる。

【0032】ステップS25では、取り出した秘密鍵46を利用者情報14を用いて復号化し、コンテンツ鍵44を再生する。ステップS26では再生したコンテンツ鍵44を用いて暗号化コンテンツ45を復号化し、ウォーターマーク入コンテンツ43をハードディスク上に展開する。ステップS27では、実際にウォーターマーク入コンテンツ43を動作させてコンテンツ利用を実行する。

【0033】〔データ運用の形態〕図9に示すような運用形態をとることも可能である。コンテンツ提供者51は、デジタルコンテンツの著作権、版權を有する版元などであり、コンテンツ管理者52にデジタルコンテンツを提供する(A)。

【0034】コンテンツ管理者52は、コンテンツ提供者51から提供されたデジタルコンテンツをコンテンツ鍵を用いて暗号化する。コンテンツ管理者52は、暗号化されたデジタルコンテンツおよびコンテンツ鍵をデータの実際の配布を行うセンター53に送信する(B)。センター53は、暗号化されたデジタルコンテンツおよびコンテンツ鍵を管理する。このセンター53は、インターネット、その他各種ネットワーク内のWEBサーバであり、ユーザ54からのアクセスに対応して、デジタルコンテンツの配布を行うように構成される。

【0035】ユーザ54は、WEBブラウザに利用してセンター53にアクセスし、データ取得のためのプラグインモジュールを取得する(C)。ユーザ54は、WEBブラウザ上でプラグインモジュールを起動し、自己の使用しているハードディスクドライブの識別番号などのユーザ固有の識別情報をセンター53に送出する(D)。センター53では、ユーザ固有の識別情報に基づいてコンテンツ鍵を暗号化して許諾情報を作成し、デジタルコンテンツのサンプルデータにウォーターマークとして埋め込み、暗号化コンテンツと合成して許諾情報入暗号化コンテンツを作成する。この許諾情報入暗号化コンテンツをコンテンツ利用者54に送信する(E)。

【0036】コンテンツ利用者54側では、受け取った許諾情報入暗号化コンテンツをハードディスクなどの利用者ディスク55に格納する(F)。デジタルコンテンツを利用する場合には、利用者ディスク55に格納されている許諾情報入暗号化コンテンツから、ユーザ固有の識別情報を用いてコンテンツ鍵を取り出し(G)、暗号化コンテンツをコンテンツ鍵で復号化してデジタルコンテンツを取り出す(H)。

【0037】このように、構成することにより、デジタルコンテンツを暗号化するためのコンテンツ鍵をコンテンツ利用者毎に変える必要がなく、1つのデジタルコンテ

10

ンツについて1つのコンテンツ鍵とすることができ、暗号鍵の管理が容易となる。また、コンテンツ利用者固有の識別情報により許諾情報のセキュリティが守られており、デジタルコンテンツの不正利用を防止することが可能となる。さらに、許諾情報が暗号化コンテンツと一体化されているため、鍵の受け渡しの手順が簡単になるとともに、暗号化コンテンツを復号化するための鍵を紛失したり破壊されたりすることがなく、鍵の再発行などの手間を省くことができる。

【0038】〔他の実施形態〕

(A) コンテンツ利用者2側で、取得した合成データを格納し、これを復号化して展開する記録媒体は、ハードディスクの他に、MO、ZIP、DVD、ICメモリ、その他のものが可能であり、その場合、利用者情報14としてこれらの装置IDを用いることができる。

【0039】(B) また、デジタルコンテンツが、CD-ROMやDVDなどの記録媒体に記録されて配布される形態の場合、パッケージ内に記載されているコンテンツIDや媒体識別番号などを利用者情報14とすることもできる。

(C) ウォーターマーク入サンプルデータ47内に埋め込まれた許諾情報には、コンテンツ利用者2がデジタルコンテンツを復号化して利用した回数を記録する領域を含むように構成できる。この場合、予め設定した回数を超えて利用しようとした場合に、これを規制するように構成することが可能である。利用した回数は、暗号化コンテンツを読み込んで復号化する際またはデジタルコンテンツの利用終了時に、利用回数を更新し、これを不可視情報としてウォーターマーク入サンプルデータ47を書き換えるように構成できる。

【0040】(D) ウォーターマーク入サンプルデータ47内に埋め込まれた許諾情報には、利用者情報14を記録する領域を含むように構成できる。この場合、デジタルコンテンツの不正コピーや不正な流通を防止できる。

(E) ウォーターマーク入サンプルデータ47内に埋め込まれた許諾情報は、複数繰り返された冗長情報とすることができる。このことにより、エラー回復機能を持たせることが可能であり、許諾情報に基づく秘密鍵46の喪失を防止することができる。

【0041】(F) ウォーターマーク入りサンプルデータ47内に埋め込まれた許諾情報は、再生できる年、月、日、時間のいずれかの範囲を規制するように構成することができる。この場合、デジタルコンテンツの不正コピーや不正な流通を防止できる。

(G) ウォーターマーク入りサンプルデータ47内に埋め込まれた許諾情報は、利用回数制御を可能とするように構成することができる。この場合、デジタルコンテンツの不正コピーや不正な流通を防止できる。

【0042】

11

【発明の効果】本発明によれば、許諾情報を含むサンプルデータ部とデジタルコンテンツを暗号化した実データ部とを一体的に合成した合成データとしてこれを配布しているため、実データ部を復号化するための鍵を実データ部と別にやりとりする必要がなく、また、ユーザ側においても実データ部と鍵とを別に管理する必要がないため、実データ部を復号化するための鍵を紛失することがなく、再発行などの煩雑な処理がなくなる。

【0043】許諾情報は、サンプルデータに不可視情報として埋め込まれているため、セキュリティを高く維持することができる。

【図面の簡単な説明】

【図1】本発明の概略構成図。

【図2】コンテンツ管理者側の概略構成図。

【図3】コンテンツ利用者側の概略構成図。

【図4】コンテンツ配布時の原理図。

【図5】コンテンツ配布時のフローチャート。

【図6】コンテンツ利用時の原理図。

【図7】コンテンツ利用時のフローチャート。

*

12

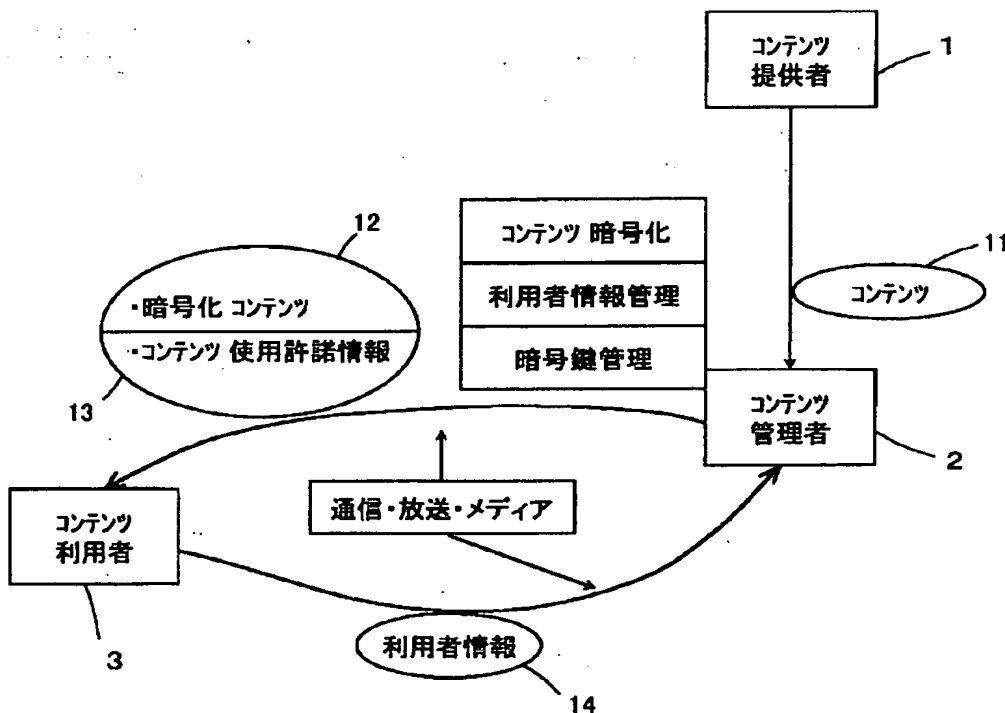
*【図8】JPEGデータの構造を示す説明図。

【図9】運用形態の1例を示す構成図。

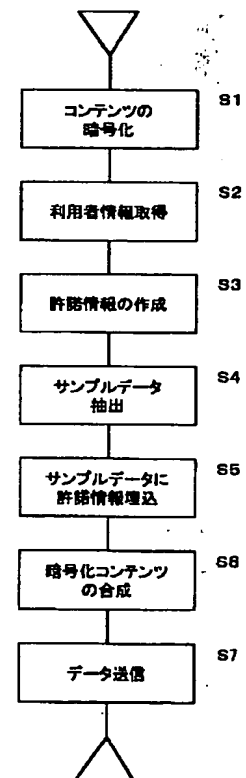
【符号の説明】

- 1 コンテンツ提供者
- 2 コンテンツ管理者
- 3 コンテンツ利用者
- 11 デジタルコンテンツ
- 12 暗号化コンテンツ
- 13 コンテンツ使用許諾情報
- 14 利用者情報
- 41 サンプルデータ
- 42 ウォーターマーク入サンプルデータ
- 43 ウォーターマーク入コンテンツ
- 44 コンテンツ鍵
- 45 暗号化コンテンツ
- 46 秘密鍵
- 47 ウォーターマーク入サンプルデータ
- 48 合成データ

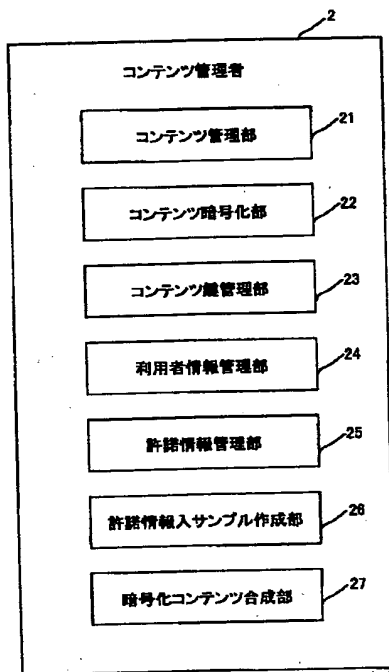
【図1】



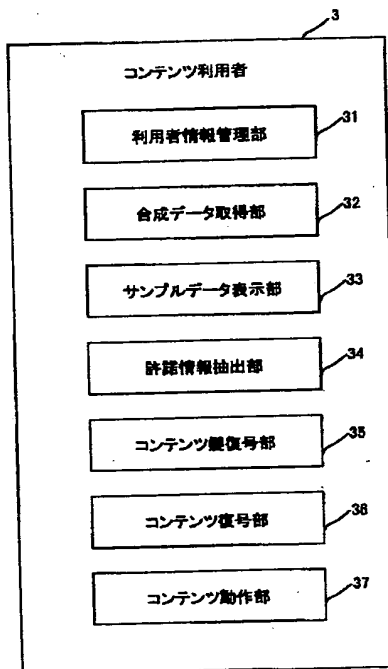
【図5】



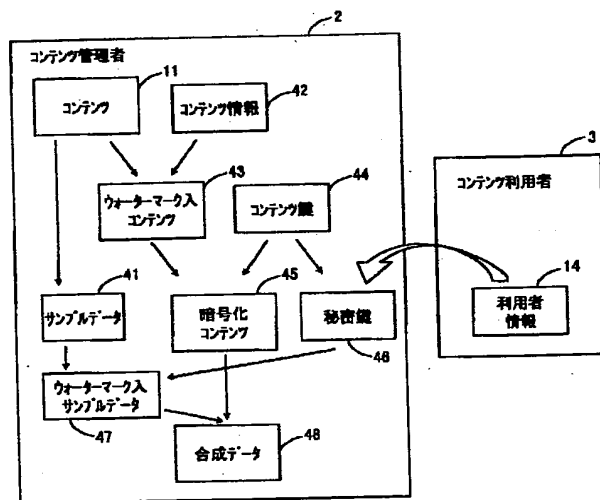
【図2】



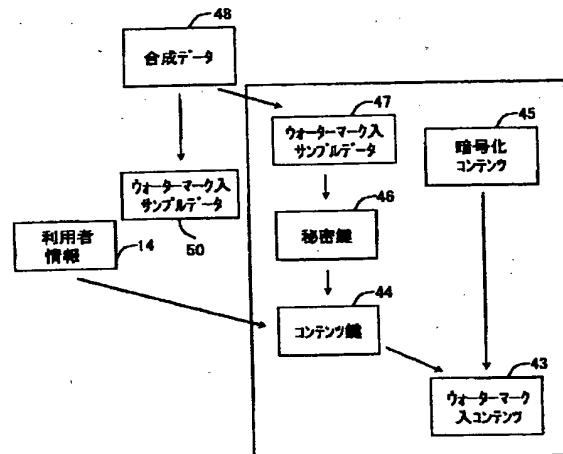
【図3】



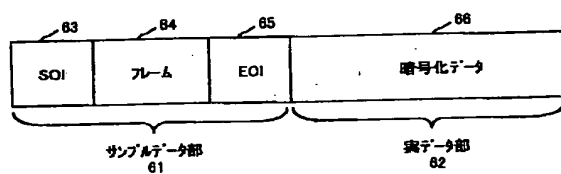
【図4】



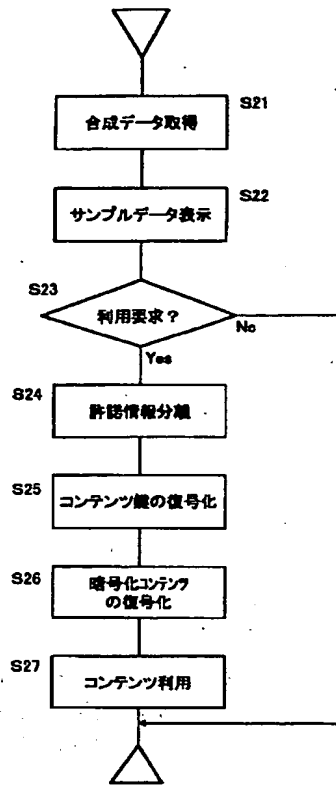
【図6】



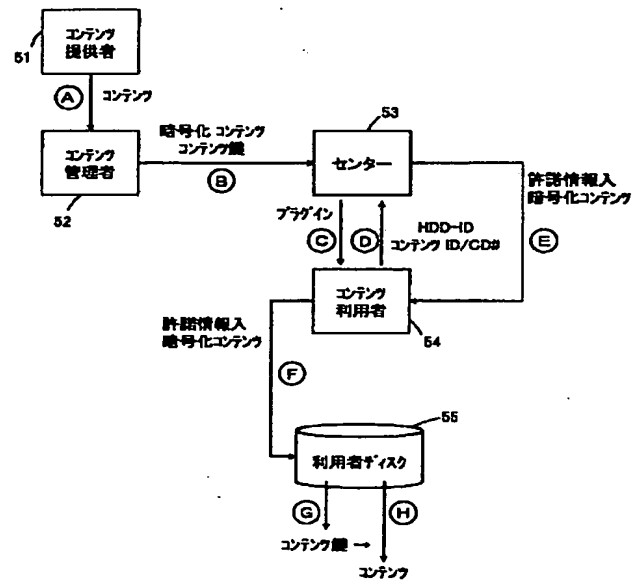
【図8】



【図7】



【図9】



フロントページの続き

(72) 発明者 橋本 晋二
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5B017 AA06 BA07 BB02 CA06 CA09
5B057 CA16 CA18 CB16 CB18 CD05
CE11 CG07
5C076 AA14

THIS PAGE BLANK (USPTO)